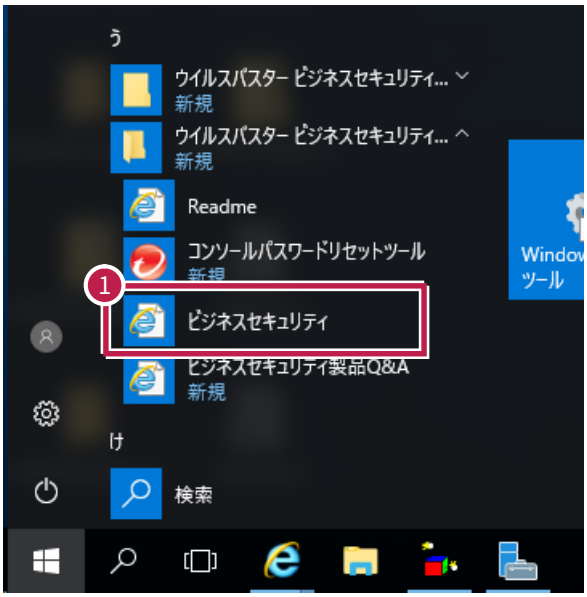
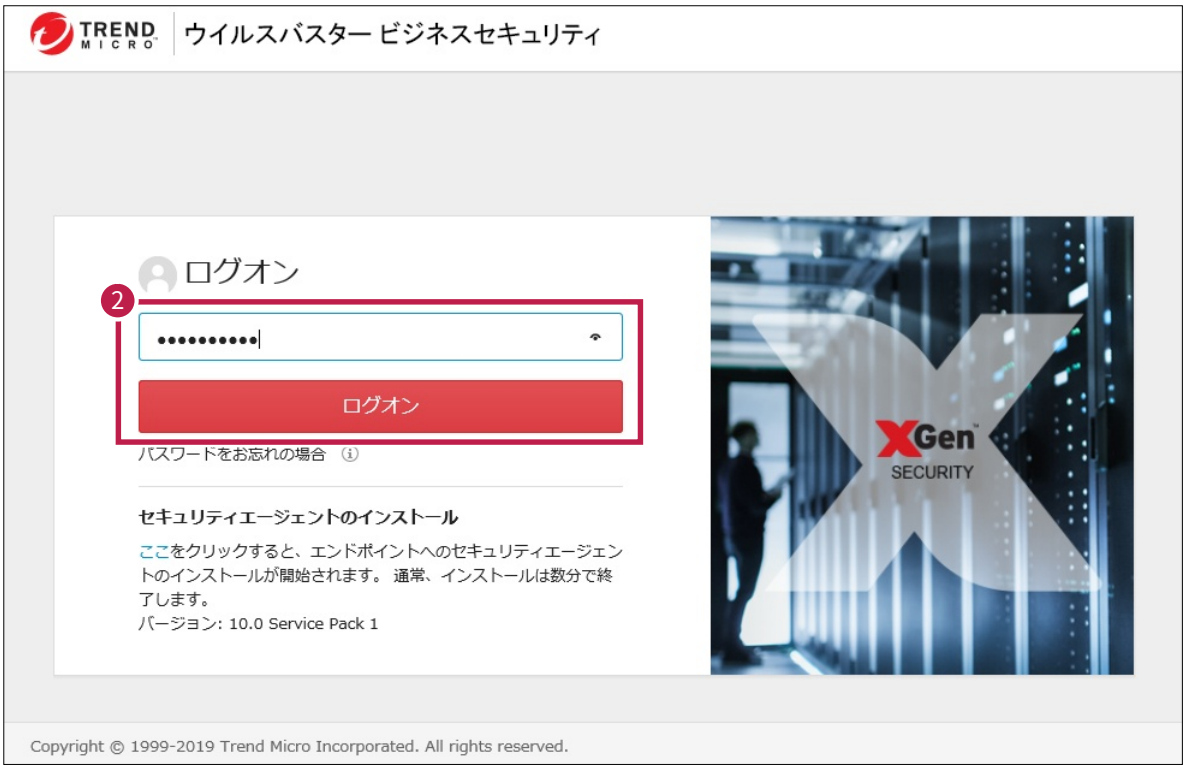
# ウィルスバスター ビジネスセキュリティ Ver10（サーバーの除外設定）

1 Windowsスタートメニューから［ビジネスセキュリティ］をクリックします。

【スタートメニュー】




2 管理者の方がパスワードを入力して、［ログオン］をクリックします。



## ① リアルタイム検索の除外設定

1 ［デバイス］ をクリックします。


2 左側のツリーから、除外設定するコンピュータグループを選択して［ポリシーの設定］ をクリックします。

3 ［ウィルス/スパイウェア対策］をクリックします。


4 ［検索対象］タブの［検索除外］の［+］をクリックします。

5 ［検索除外を有効にする］がONであることを確認します。

6 弊社製品がインストールされているフォルダーパス「**C**:¥FCAPP」を入力します。
（**C**は弊社製品のインストールドライブです。お客様の環境に合わせて読み替えてください。）
※参照ツリーなどは表示されないので、手入力する必要があります。
※指定したフォルダーのサブフォルダーも除外対象となります。

7 ［追加］ボタンをクリックします。


8 下部のリストに、フォルダーパスが追加されたことを確認します。

9 以下のフォルダーが存在する場合は、同様な手順で、それぞれリストに追加してください。
※存在しない場合は追加不要です。
・32 ビットOS の場合「C:¥Program Files ¥Common Files¥Fukui Computer Shared」
・64 ビットOS の場合「C:¥Program Files (x86)¥Common Files¥Fukui Computer Shared」


10 追加が終わったら、下にスクロールして［保存］をクリックします。

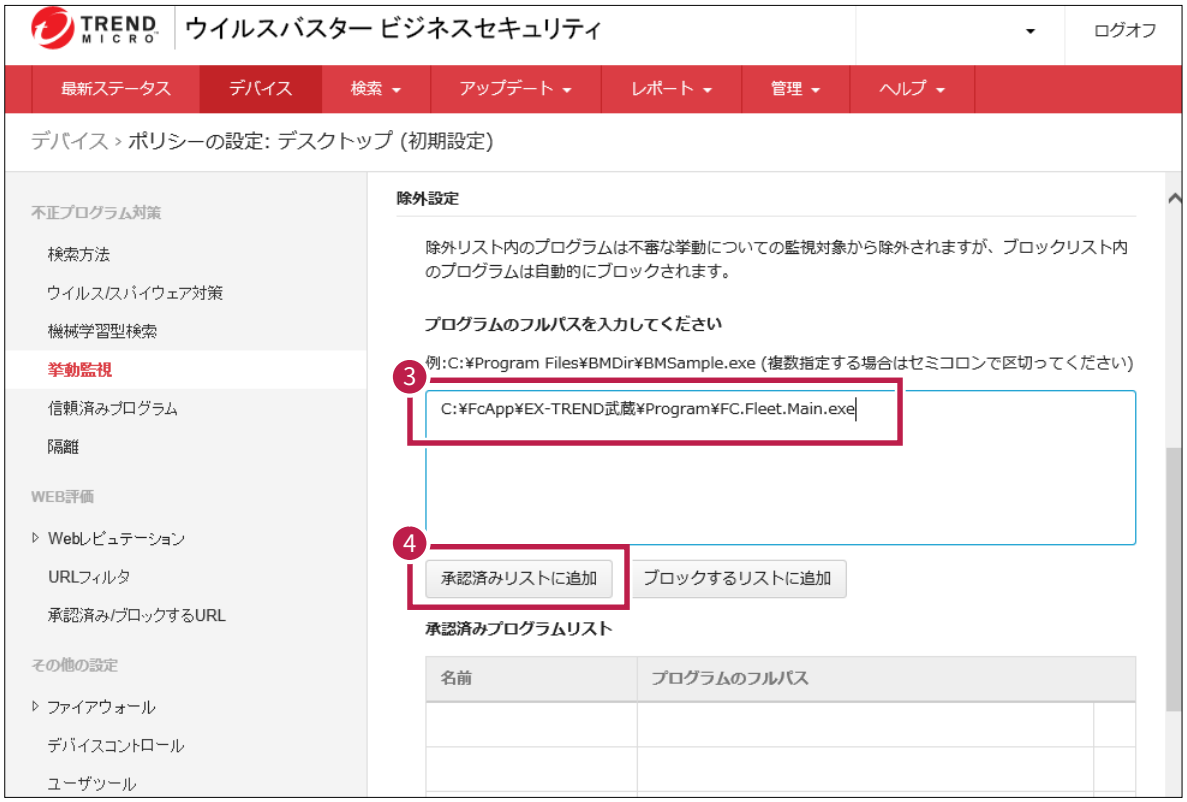
## ② 挙動監視の除外設定／信頼済みプログラムに追加

1 ［挙動監視］、または［信頼済みプログラム］をクリックします。
※ここでは［挙動監視］で記載しますが、［信頼済みプログラム］も設定方法は同じです。
ただし、［信頼済みプログラム］に有効化･無効化の設定はありません。


2 ［挙動監視の有効化］がONであることを確認します。

3 下にスクロールして［除外設定］のボックスに、「C:¥FCAPP」フォルダー内のexeファイルのパスを手入力します。
例：**C**:¥FcApp¥EX-TREND武蔵¥Program¥FC.Fleet.Main.exe
（**C**は弊社製品のインストールドライブです。お客様の環境に合わせて読み替えてください。）
※その他の除外設定するexeファイルは、P.9を参照してください。

4 ［承認済みリストに追加］をクリックします。




5 ［承認済みプログラムリスト］に追加されたことを確認します。

6 同様な手順で、必要なファイルをすべてリストに追加してください。

7 追加が終わったら、［保存］をクリックします。

# EX-TREND 武蔵に関して除外設定をおすすめする EXE ファイル一覧

（ウィルスとして誤認識された場合に、除外設定の参考にしてください。）

| EX-TREND 武蔵 | | | |
|---|---|---|---|
| No | EXE ファイルが存在するフォルダーパス | EXE ファイル名 | 関係するプログラム |
| 1 | C:¥FCAPP¥EX-TREND 武蔵¥Program | FC.Fleet.Main.exe | インデックス |
| 2 | | FC.Procedure.Main.exe | 施工計画書作成支援 |
| 3 | | CCad.exe | 建設 CAD |
| 4 | | FC.Scheduler.exe | 工程管理 |
| 5 | | FC.CsManager.exe | 原価工程管理 |
| 6 | | ExPhoto.exe | 写真管理 |
| 7 | | ExAlbum.exe | アルバム編集 |
| 8 | | ExDeki.exe | 出来形管理 |
| 9 | | ExPave.exe | 舗装出来形管理 |
| 10 | | ExQual.exe | アスファルト温度管理 |
| 11 | | | コンクリート品質管理 |
| 12 | | TrndEnou.exe | 電子納品ツール |
| 13 | C:¥FCAPP¥FCNCLCenter | FCNCLCenter.exe | ネット認証ライセンスセンター |
| 14 | C:¥FCAPP¥Concierge¥Program | TRENDLive.exe | FC コンシェルジュ |

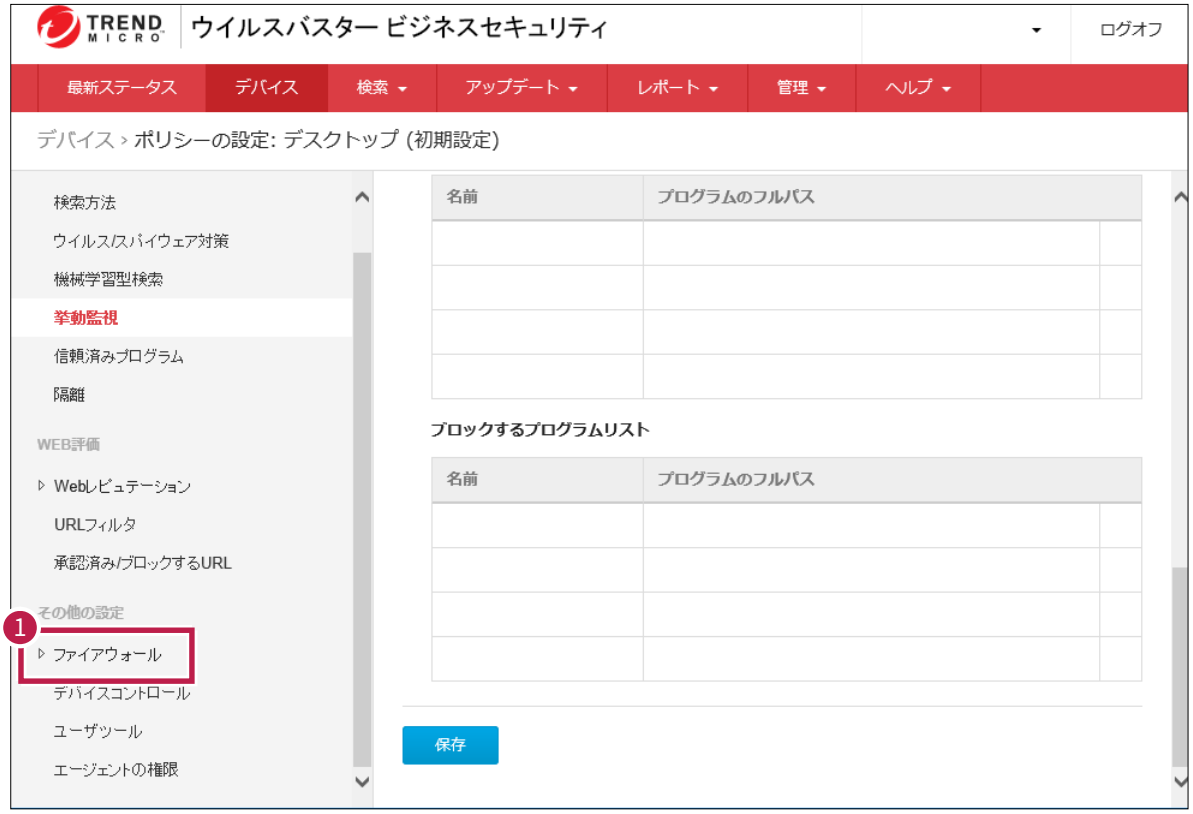
※**C**は弊社製品のインストールドライブです。お客様の環境に合わせて読み替えてください。

※弊社の他プログラムでも、ウィルスとして誤認識される場合があります。
　その時は各プログラム（program）フォルダー内の誤認識された EXE ファイルを除外設定して下さい。
例）
・TREND-ONE の場合 「C:¥FCAPP¥TREND-ONE¥Program」フォルダー以下の EXE ファイル
・BTXA の場合 「C:¥FCAPP¥BTXA¥Program」フォルダー以下の EXE ファイル

## ③ ファイアウォールの除外設定

SNSーLANプロテクト、またはTREND-ONE、Mercury-ONE、BLUETREND XAの共同編集機能をご利用のお客様は［ファイアウォール］に除外設定をしてください。その他のお客様は設定の必要はありません。

**1** ［ファイアウォール］をクリックします。




**2** ［オフィス内］の［ファイアウォールを有効にする］がONで、［詳細モード］であることを確認してください。

3 下にスクロールして、［除外設定］の［追加］をクリックします。


4 下表に従って設定します。画像は、「SNS－LAN」 の設定内容になっています。

| 名前 | 処理 | 方向 | プロトコル | ポート | コンピュータ |
|---|---|---|---|---|---|
| SNS－LAN | 許可 | 送受信 | UDP | 指定：5093 | すべての IP アドレス |
| SQL Server Express | 許可 | 受信 | TCP | 指定：1435 | すべての IP アドレス |
| SQL Browser | 許可 | 受信 | UDP | 指定：1434 | すべての IP アドレス |
| MTS | 許可 | 送受信 | TCP | 指定：8103 | すべての IP アドレス |

5 下にスクロールして、［保存］をクリックします。


6 リストに追加されたことを確認します。

7 同様な手順で、必要な設定をすべて追加してください。追加が完了したら、［保存］をクリックします。

## ④ 手動検索／予約検索の除外設定

**1** ［検索］ー［手動検索］、または［予約検索］をクリックします。
※ここでは［手動検索］で記載しますが、［予約検索］も設定方法は同じです。


**2** 除外設定するコンピュータグループをクリックします。

3 ［検索除外］の［+］をクリックします。


4 ［検索除外を有効にする］がONであることを確認します。

5 弊社製品がインストールされているフォルダーパス「**C**:¥FCAPP」を入力します。
（**C**は弊社製品のインストールドライブです。お客様の環境に合わせて読み替えてください。）
※参照ツリーなどは表示されないので、手入力する必要があります。
※指定したフォルダーのサブフォルダーも除外対象となります。

6 ［追加］ボタンをクリックします。

7 下部のリストに、フォルダーパスが追加されたことを確認します。


8 以下のフォルダーが存在する場合は、同様な手順で、それぞれリストに追加してください。
※存在しない場合は追加不要です。
・32 ビットOS の場合「C:¥Program Files ¥Common Files¥Fukui Computer Shared」
・64 ビットOS の場合「C:¥Program Files (x86)¥Common Files¥Fukui Computer Shared」

9 追加が終わったら、下にスクロールして［保存］をクリックします。
以上で終了です。